

1 Общие замечания

Данный текст представляет из себя краткий конспект лекций по курсу «Математическая логика», рассказанных студентам ИТМО (группы 2537-2539) в 2012-2013 учебном году.

2 Исчисление высказываний

Матлогика — это наука о правильных математических рассуждениях, а поскольку рассуждения обычно ведутся на каком-то языке, то она неразрывна связана с идеей двух языков: *языка исследователя* (или иначе его называют *мета-языком*), и *предметного языка*. Как следует из названий, языком исследователя пользуемся мы, формулируя утверждения или доказывая теоремы о разных способах математических рассуждений, или просто их обсуждая. Сами же математические рассуждения, собственно и составляющие предмет исследования, формализованы в некотором предметном языке.

Мы начнём с очень простого предметного языка — языка исчисления высказываний. Элементами (строками) данного языка являются некоторые выражения (формулы), по структуре очень похожие на арифметические, которые называются *высказываниями*.

Каждое высказывание — это либо *пропозициональная переменная* — большая буква латинского алфавита, возможно, с цифровым индексом, либо оно составлено из одного или двух высказываний меньшего размера, соединённых логической связкой.

Связок в языке мы определим 4 (хотя при необходимости этот список может быть в любой момент изменён).

- конъюнкция: если $\alpha\beta$ — высказывания, то $\alpha\&\beta$ — тоже высказывание.
- дизъюнкция: если $\alpha\beta$ — высказывания, то $\alpha\vee\beta$ — тоже высказывание.
- импликация: если $\alpha\beta$ — высказывания, то $\alpha\rightarrow\beta$ — тоже высказывание.
- отрицание: если α — высказывание, то $\neg\alpha$ — тоже высказывание.

Высказывания, подробности которых нас не интересуют, мы будем обозначать начальными буквами греческого алфавита (α , β , γ и т.п.).

2.1 Оценка высказываний

Процесс «вычисления» значения высказываний (*оценка высказываний*) имеет совершенно естественное определение. Мы фиксируем некоторое множество *истинностных значений*, для начала мы в качестве такого множества возьмем множество $\{\text{И}, \text{Л}\}$, здесь И означает истину, а Л — ложь. Всем пропозициональным переменным мы приписываем некоторое значение, а затем рекурсивно вычисляем значение выражения естественным для указанных связок образом.

В дальнейшем мы будем брать необычные множества истинностных значений, и будем давать неожиданный смысл связкам, однако, классическая интерпретация связок является традиционной и всегда подразумевается, если не указано иного.

Среди высказываний выделяются те, что остаются истинными при любой оценке пропозициональных переменных. Такие высказывания называют *тавтологиями* или *общезначимыми высказываниями*. Также, на языке исследователя общезначимость высказывания α можно кратко записать как $\models \alpha$.

2.2 Доказательства

В любой теории есть некоторые утверждения (аксиомы), которые принимаются без доказательства. В исчислении высказываний мы должны явно определить список всех возможных аксиом. Например, мы можем взять утверждение $A \& B \rightarrow A$ в качестве аксиомы. Однако, у него есть множество аналогичных утверждений, например, $B \& A \rightarrow B$, которые не отличаясь по сути, отличаются по записи, и формально говоря, являются другим утверждением.

Для решения вопроса мы введём понятие *схемы аксиом* — некоторого обобщённого шаблона, подставляя значения в который, мы получаем различные, но схожие аксиомы. Например, схема аксиом $\psi \& \phi \rightarrow \psi$ позволяет получить как аксиому $A \& B \rightarrow A$ (при подстановке $\psi := A, \phi := B$), так и аксиому $B \& A \rightarrow B$.

Возьмем следующие схемы аксиом для исчисления высказываний.

- (1) $(\phi) \rightarrow ((\psi) \rightarrow (\phi))$
- (2) $((\phi) \rightarrow (\psi)) \rightarrow ((\phi) \rightarrow (\psi) \rightarrow (\pi)) \rightarrow ((\phi) \rightarrow (\pi))$
- (3) $(\phi) \rightarrow (\psi) \rightarrow (\phi) \& (\psi)$
- (4) $(\phi) \& (\psi) \rightarrow (\phi)$
- (5) $(\phi) \& (\psi) \rightarrow (\psi)$
- (6) $(\phi) \rightarrow (\phi) \vee (\psi)$
- (7) $(\psi) \rightarrow (\phi) \vee (\psi)$
- (8) $((\phi) \rightarrow (\pi)) \rightarrow ((\psi) \rightarrow (\pi)) \rightarrow ((\phi) \vee (\psi) \rightarrow (\pi))$
- (9) $((\phi) \rightarrow (\psi)) \rightarrow ((\phi) \rightarrow \neg(\psi)) \rightarrow \neg(\phi)$
- (10) $\neg\neg(\phi) \rightarrow (\phi)$

Помимо аксиом, нам требуется каким-то образом научиться преобразовывать одни верные утверждения в другие. Сделаем это с помощью правил вывода. У нас пока будет одно правило вывода — *Modus Ponens*. Это также схема, она позволяет при доказанности двух формул ψ и $\psi \rightarrow \phi$ считать доказанной формулу ϕ .

Определение 2.1. *Доказательство* в исчислении высказываний — это некоторая конечная последовательность выражений $\alpha_1, \alpha_2 \dots \alpha_n$ из языка L , такая, что каждое из утверждений $\alpha_i (1 \leq i \leq n)$ либо является аксиомой, либо получается из других утверждений $\alpha_{P_1}, \alpha_{P_2} \dots \alpha_{P_k} (P_1 \dots P_k < i)$ по правилу вывода.

Определение 2.2. Высказывание α называется доказуемым, если существует доказательство $\alpha_1, \alpha_2 \dots \alpha_k$, и в нем α_k совпадает с α .

Вообще, схемы аксиом и правила вывода существуют для удобства задания исчисления. В дальнейшем будет очень неудобно возиться с этими объектами. Поэтому мы считаем, что в исчислении имеется бесконечно много аксиом и правил вывода, которые порождаются подстановкой всех возможных формул вместо параметров в схемы.

В качестве сокращения записи в языке исследователя мы будем писать $\vdash \alpha$, чтобы сказать, что α доказуемо.

Традиционно правила вывода записывают так:

$$\frac{\phi \quad (\phi) \rightarrow (\psi)}{\psi}$$

3 Теорема о дедукции

Соглашение об обозначениях. Будем обозначать буквами $\Gamma, \Delta, \Sigma, \Pi$ списки формул (возможно, пустые).

Определение 3.1. Вывод из допущений. Пусть Γ – некоторый список высказываний, а α – некоторое высказывание. Тогда мы будем говорить, что высказывание α *выводимо* из Γ (и записывать это как $\Gamma \vdash \alpha$), если существует такая последовательность высказываний $\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \alpha$ (называемая *выводом* α из Γ), что каждое из высказываний α_i – это

- либо аксиома,
- либо получается по правилу Modus Ponens из предыдущих высказываний,
- либо – высказывание из списка Γ .

Элементы Γ мы будем называть *допущениями*. Также эти элементы называют предположениями или гипотезами.

В свете данного определения можно заметить, что доказательство – это вывод из пустого списка допущений.

Теорема 3.1. Теорема о дедукции. Утверждение $\Gamma \vdash \alpha \rightarrow \beta$ справедливо тогда и только тогда, когда справедливо, что $\Gamma, \alpha \vdash \beta$.

Для доказательства рассмотрим следующую лемму:

Лемма 3.2. $\vdash \alpha \rightarrow \alpha$

Доказательство.

- | | |
|--|------------|
| (1) $\alpha \rightarrow (\alpha \rightarrow \alpha)$ | Сх. акс. 1 |
| (2) $(\alpha \rightarrow (\alpha \rightarrow \alpha)) \rightarrow (\alpha \rightarrow ((\alpha \rightarrow \alpha) \rightarrow \alpha)) \rightarrow (\alpha \rightarrow \alpha)$ | Сх. акс. 2 |
| (3) $(\alpha \rightarrow ((\alpha \rightarrow \alpha) \rightarrow \alpha)) \rightarrow (\alpha \rightarrow \alpha)$ | М.Р. 1,2 |
| (4) $(\alpha \rightarrow ((\alpha \rightarrow \alpha) \rightarrow \alpha))$ | Сх. акс. 1 |
| (5) $\alpha \rightarrow \alpha$ | М.Р. 4,3 |

□

Доказательство теоремы ??. Сперва докажем прямое следствие. Для этого нам достаточно научиться по любому выводу $\alpha \rightarrow \beta$ из Γ строить вывод β из Γ, α . Возьмем вывод формулы $\alpha \rightarrow \beta$, то есть некоторую последовательность формул $\delta_1 \dots \delta_{m-1}; \alpha \rightarrow \beta$. Добавив к выводу 2 формулы, получаем требуемый вывод:

- | | |
|------------------------------------|----------------------------|
| (1) δ_1 | |
| ... | |
| ($m-1$) δ_{m-1} | |
| (m) $\alpha \rightarrow \beta$ | |
| ($m+1$) α | «Свежедобавленная» аксиома |
| ($m+2$) β | М.Р. $m, m+1$ |

Теперь докажем обратное. Нам необходимо построить вывод утверждения $\Gamma \vdash \alpha \rightarrow \beta$ по имеющемуся выводу $\delta_1 \dots \delta_{m-1}, \beta$. Мы поступим так: сперва набросаем план вывода – разместим по тексту «ключевые» формулы, которые потом дополним до полноценного вывода промежуточными формулами.

План вывода будет такой:

- | |
|---|
| (1) $\Gamma \vdash \alpha \rightarrow \delta_1$ |
| ... |
| ($m-1$) $\Gamma \vdash \alpha \rightarrow \delta_{m-1}$ |
| (m) $\Gamma \vdash \alpha \rightarrow \beta$ |

Теперь надо дополнить его до полноценного вывода. Будем рассматривать формулы подряд и перед каждой формулой добавлять некоторое количество формул, обосновывающих соответствующий шаг доказательства. Рассмотрим формулу номер i . Возможны следующие варианты:

1. δ_i — это аксиома или предположение, входящее в Γ . Тогда перед этой формулой вставим формулы δ_i и $\delta_i \rightarrow (\alpha \rightarrow \delta_i)$, и окажется, что i -я формула выводится из предыдущих двух формул путем применения правила Modus Ponens.
2. δ_i совпадает с α . Тогда мы вставим перед ней 4 первые формулы из леммы, и $\delta_i \rightarrow \alpha$ будет получаться по правилу Modus Ponens.
3. δ_i выводится по правилу Modus Ponens из каких-то других утверждений δ_j и δ_k (при этом $\delta_k \equiv \delta_j \rightarrow \delta_i$), где $j < i$ и $k < i$. Покажем, что $\alpha \rightarrow \delta_i$ тоже может быть выведена из утверждений $\alpha \rightarrow \delta_j$ и $\alpha \rightarrow (\delta_j \rightarrow \delta_i)$.

Для этого добавим два высказывания:

$$\begin{array}{ll} (\alpha \rightarrow \delta_j) \rightarrow ((\alpha \rightarrow (\delta_j \rightarrow \delta_i)) \rightarrow (\alpha \rightarrow \delta_i)) & \text{Сх. акс. 2} \\ ((\alpha \rightarrow (\delta_j \rightarrow \delta_i)) \rightarrow (\alpha \rightarrow \delta_i)) & \text{М.Р. из } j \text{ и } i - 6 \end{array}$$

□

По аналогии мы можем рассмотреть отношение *следования*. Будем говорить, что высказывание α следует из высказываний Γ , если при любой оценке пропозициональных переменных, входящих в высказывания Γ и α , на которых все высказывания из Γ истинны, α также истинно. Записывать, что α следует из Γ , будем так: $\Gamma \models \alpha$.

4 Теорема о полноте исчисления высказываний

Определение 4.1. Введем обозначение. Пусть α — это некоторое высказывание, а x — некоторое истинностное значение. Тогда обозначим за $[x]\alpha$ высказывание α , если x — истина, и $\neg(\alpha)$, если x — ложь. Также, если формула α — это формула с n пропозициональными переменными $P_1 \dots P_n$, и $x_1 \dots x_n$ — некоторые истинностные значения, то за $\llbracket \alpha \rrbracket^{P_1:=x_1, \dots, P_n:=x_n}$ обозначим значение формулы α при подстановке значений $x_1 \dots x_n$ вместо переменных $P_1 \dots P_n$.

Лемма 4.1. Если $\Gamma, \Sigma \vdash \alpha$, то $\Gamma, \Delta, \Sigma \vdash \alpha$. Если $\Gamma, \Delta, \Sigma, \Pi \vdash \alpha$, то $\Gamma, \Sigma, \Delta, \Pi \vdash \alpha$.

Доказательство. Упражнение

□

Лемма 4.2. Если справедливы 3 утверждения: $\Gamma \vdash \gamma$, $\Delta \vdash \delta$ и $\gamma, \delta \vdash \alpha$, то справедливо и $\Gamma, \Delta \vdash \alpha$

Доказательство. Мы получим требуемый вывод, просто последовательно соединив все три исходных вывода. Первые два вывода будут (очевидно) корректными при допущениях Γ и Δ . В третьем же выводе могут использоваться высказывания γ и δ , отсутствующие в предположениях. Но поскольку эти высказывания доказаны в первых двух частях вывода, мы будем иметь полное право их упоминать — на тех же основаниях, на которых они указаны в конце соответствующих доказательств.

□

Возьмем некоторую связку исчисления высказываний, например конъюнкцию: $A \& B$. Построим для нее таблицу истинности. По каждой строчке построим утверждение, в котором отрицания появляются там, где в таблице истинности находится L :

A	B	$A \& B$	утверждение
Л	Л	Л	$\neg A, \neg B \vdash \neg(A \& B)$
Л	И	Л	$\neg A, B \vdash \neg(A \& B)$
И	Л	Л	$A, \neg B \vdash \neg(A \& B)$
И	И	И	$A, B \vdash A \& B$

Лемма 4.3. Каждое из построенных по таблицам истинности утверждений доказуемо.

Доказательство. Упражнение. □

Лемма 4.4 (Правило контрапозиции). Каковы бы ни были формулы α и β , справедливо, что $\vdash (\alpha \rightarrow \beta) \rightarrow (\neg\beta \rightarrow \neg\alpha)$

Доказательство. Сперва докажем, что $\alpha \rightarrow \beta, \neg\beta \vdash \neg\alpha$.

- (1) $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \neg\beta) \rightarrow \neg\alpha$ Сх. акс. 8
- (2) $\alpha \rightarrow \beta$ Допущение
- (3) $(\alpha \rightarrow \neg\beta) \rightarrow \neg\alpha$ М.Р. 2,1
- (4) $\neg\beta \rightarrow (\alpha \rightarrow \neg\beta)$ Сх. акс. 1
- (5) $\neg\beta$ Допущение
- (6) $\alpha \rightarrow \neg\beta$ М.Р. 5,4
- (7) $\neg\alpha$ М.Р. 6,3

Тогда, применив 2 раза Теорему о дедукции, получим вывод требуемого утверждения. □

Лемма 4.5. Правило исключенного третьего. Какова бы ни была формула α , $\vdash \alpha \vee \neg\alpha$

Доказательство. Доказательство проведем в 3 этапа.

1. Для начала покажем $\vdash \neg(\alpha \vee \neg\alpha) \rightarrow \neg\alpha$:

- (1) $\alpha \rightarrow \alpha \vee \neg\alpha$ Сх. акс. 6
- (2) $\dots (n+1)$ $\gamma_1, \dots, \gamma_{n-1}, (\alpha \rightarrow \alpha \vee \neg\alpha) \rightarrow (\neg(\alpha \vee \neg\alpha) \rightarrow \neg\alpha)$ Д-во из леммы ??
- (n+2) $\neg(\alpha \vee \neg\alpha) \rightarrow \neg\alpha$ М.Р. 1, n+1

2. Затем докажем $\vdash \neg(\alpha \vee \neg\alpha) \rightarrow \neg\neg\alpha$:

- (1) $\neg\alpha \rightarrow \alpha \vee \neg\alpha$ Сх. акс. 7
- (2) $\dots (k+1)$ $\delta_1, \dots, \delta_{k-1}, (\neg\alpha \rightarrow \alpha \vee \neg\alpha) \rightarrow (\neg(\alpha \vee \neg\alpha) \rightarrow \neg\neg\alpha)$ Д-во из леммы ??
- (k+2) $\neg(\alpha \vee \neg\alpha) \rightarrow \neg\neg\alpha$ М.Р. 1, k+1

3. Теперь докажем все вместе:

- (1) $\neg(\alpha \vee \neg\alpha) \rightarrow \neg\alpha$ по пункту 1
- (2) $\neg(\alpha \vee \neg\alpha) \rightarrow \neg\neg\alpha$ по пункту 2
- (3) $(\neg(\alpha \vee \neg\alpha) \rightarrow \neg\alpha) \rightarrow (\neg(\alpha \vee \neg\alpha) \rightarrow \neg\neg\alpha) \rightarrow (\neg\neg(\alpha \vee \neg\alpha))$ Сх. акс. 9
- (4) $(\neg(\alpha \vee \neg\alpha) \rightarrow \neg\neg\alpha) \rightarrow \neg\neg(\alpha \vee \neg\alpha)$ М.Р. 1,3
- (5) $\neg\neg(\alpha \vee \neg\alpha)$ М.Р. 2,4
- (6) $\neg\neg(\alpha \vee \neg\alpha) \rightarrow (\alpha \vee \neg\alpha)$ Сх. акс. 10
- (7) $\alpha \vee \neg\alpha$ М.Р. 5,6

□

Лемма 4.6. Об исключении допущения. Пусть справедливо $\Gamma, \rho \vdash \alpha$ и $\Gamma, \neg\rho \vdash \alpha$. Тогда также справедливо $\Gamma \vdash \alpha$.

Доказательство. Применив теорему о дедукции к условиям теоремы получим следующее:

$$\Gamma \vdash \rho \rightarrow \alpha$$

$$\Gamma \vdash \neg \rho \rightarrow \alpha$$

Тогда следующий вывод покажет $\Gamma \vdash \alpha$:

(1) ... (p)	$\gamma_1, \dots, \gamma_{p-1}, \rho \rightarrow \alpha$	Вывод $\Gamma \vdash \rho \rightarrow \alpha$
(p + 1) ... (q)	$\delta_1, \dots, \delta_{q-p-1}, \neg \rho \rightarrow \alpha$	Вывод $\Gamma \vdash \neg \rho \rightarrow \alpha$
(q + 1) ... (r)	$\epsilon_1, \dots, \epsilon_{r-q-1}, \rho \vee \neg \rho$	Лемма ??
(r + 1)	$(\rho \rightarrow \alpha) \rightarrow (\neg \rho \rightarrow \alpha) \rightarrow (\rho \vee \neg \rho) \rightarrow \alpha$	Сх. аксиом 8
(r + 2)	$(\neg \rho \rightarrow \alpha) \rightarrow (\rho \vee \neg \rho \rightarrow \alpha)$	М.Р. 1, r + 1
(r + 3)	$\rho \vee \neg \rho \rightarrow \alpha$	М.Р. p, r + 2
(r + 4)	α	М.Р. r, r + 3

□

Теорема 4.7. О полноте исчисления высказываний. Пусть справедливо $\models \alpha$. Тогда также справедливо, что $\vdash \alpha$.

Доказательство. Для доказательства теоремы мы докажем чуть более сильное утверждение — что для любого k от 0 до n и любой оценки переменных x_1, \dots, x_k справедливо ${}_{[x_1]}P_1, \dots, {}_{[x_k]}P_k \vdash \alpha$. Нетрудно заметить, что утверждение теоремы непосредственно следует из данного утверждения для $k = 0$. Доказательство будет вестись индукцией по $n - k$.

База. Пусть $n - k = 0$, то есть $k = n$. $\models \alpha$ означает, что при любой оценке x_1, \dots, x_n пропозициональных переменных P_1, \dots, P_n справедливо $\alpha[P_1 := x_1, \dots, P_n := x_n] = \text{И}$. Возьмем некоторую оценку переменных x_1, \dots, x_n . Тогда, по лемме ??, ${}_{[x_1]}P_1, \dots, {}_{[x_n]}P_n \vdash \alpha[P_1 := x_1, \dots, P_n := x_n]\alpha$ то есть ${}_{[x_1]}P_1, \dots, {}_{[x_n]}P_n \vdash \alpha$.

Переход. Пусть утверждение уже доказано для некоторого $n - k > 0$, покажем его для $n - k + 1$ (то есть доказано для $k < n$, покажем его для $k + 1$). Возьмем некоторую оценку переменных x_1, \dots, x_{k-1} . По предположению, ${}_{[x_1]}P_1, \dots, {}_{[x_k]}P_k \vdash \alpha$, то есть

$${}_{[x_1]}P_1, \dots, {}_{[x_{k-1}]}P_{k-1}, \neg P_k \vdash \alpha$$

$${}_{[x_1]}P_1, \dots, {}_{[x_{k-1}]}P_{k-1}, P_k \vdash \alpha$$

Тогда по лемме об исключении допущения, справедливо ${}_{[x_1]}P_1, \dots, {}_{[x_{k-1}]}P_{k-1} \vdash \alpha$.

□

Теорема 4.8. О корректности исчисления высказываний. Пусть справедливо $\vdash \alpha$. Тогда также справедливо, что $\models \alpha$.

Доказательство. По условию теоремы, у нас есть доказательство высказывания α , то есть последовательность высказываний $\alpha_1, \dots, \alpha_m$. Каждое высказывание — это либо аксиома, либо применение правила Modus Ponens. Докажем, что для каждого k все высказывания α_l при $l \leq k$ — тавтологии. Доказательство будем вести индукцией по k .

База. Пусть $k = 0$, тогда нет ни одного высказывания, про которое нужно доказать, что оно — тавтология, то есть утверждение автоматически верно.

Переход. Пусть для некоторого k утверждение справедливо, докажем его для $k + 1$. Выберем некоторую оценку x_1, \dots, x_n пропозициональных переменных P_1, \dots, P_n , использованных в высказываниях $\alpha_1 \dots \alpha_{k+1}$. Рассмотрим случаи.

Пусть α_{k+1} — аксиома. В данную аксиому входят одна, две или три формулы $\beta_1, \beta_2, \beta_3$. Подставив всех возможных истинностных значений вместо данных формул можно проверить, что все аксиомы являются тавтологиями, значит, они будут истинны и на тех конкретных значениях, которые примут данные формулы после подстановки значений x_1, \dots, x_n .

Пусть α_{k+1} получается по правилу Modus Ponens из α_p и α_q , причем $\alpha_q \equiv \alpha_p \rightarrow \alpha_{k+1}$. Тогда $\alpha_p[x_1, \dots, x_n] = \text{И}$ и $(\alpha_p \rightarrow \alpha_{k+1})[x_1, \dots, x_n] = \text{И}$. Из таблицы истинности импликации следует, что неизбежно $\alpha_{k+1}[x_1, \dots, x_n] = \text{И}$.

□

Заметим, что вместе из этих двух теорем следует, что если неверно, что $\vdash \alpha$, то неизбежно найдется контрпример.

5 Интуиционистское исчисление высказываний

Заменяем аксиому устранения двойного отрицания на $\phi \rightarrow \neg\phi \rightarrow \psi$. Полученная система называется интуиционистским исчислением высказываний.

Теорема 5.1. В интуиционистском исчислении высказываний невозможно доказать правило исключенного третьего: $P \vee \neg P$.

Мы рассмотрим *модельное* доказательство. То есть, мы построим некоторую модель для исчисления высказываний — так определим истинностные значения и связки, что в нем правило исключенного третьего перестанет быть тавтологией, при этом построенная нами модель останется корректной.

Пусть множество истинностных значений будет состоять из трех элементов: И, Н и Л. Определим отношение порядка, будем считать, что $I > N > L$.

Все связки на истине и лжи действуют традиционно, необходимо описать только их поведение с элементом Н. Для двух операций дадим естественные обобщения. $A \& B = \min(A, B)$, $A \vee B = \max(A, B)$. Однако, положим $\neg N = L$. Также, операцию $A \rightarrow B$ положим $\neg A \vee B$, за исключением $N \rightarrow N = I$.

Будем считать, что высказывание истинно на некоторой оценке, если оно на ней принимает значение И. Общезначимость же ($\models \alpha$) означает, что $\alpha[x_1, \dots, x_n] = I$ для любой оценки переменных x_1, \dots, x_n .

Нетрудно показать, что так определенная модель исчисления является корректной — то есть любое утверждение, имеющее доказательство, является тавтологией в смысле данной модели.

Доказательство теоремы ??. Поскольку $N \vee \neg N = N$, то в данной модели неверно $\models P \vee \neg P$. Значит, если бы существовало доказательство этого утверждения, то рассмотренная модель была бы некорректной. Значит, для интуиционистского исчисления высказываний неверно $\vdash P \vee \neg P$. \square

Однако, так построенная логика (с такой моделью) не является полной. Например, высказывание $\neg P \vee \neg\neg P$, не являющееся доказуемым в интуиционистской логике, тем не менее оказывается истинным. Сейчас мы рассмотрим другие модели, обладающие свойством полноты.

5.1 Топологическая интерпретация интуиционистского исчисления высказываний

Пусть дано некоторое исчисление высказываний, для которого нам нужно построить модель — предложить способ оценки истинности выражений. Начинаем мы с множества истинностных значений. Возьмем в качестве этого множества все открытые множества некоторого заранее выбранного топологического пространства. Определим оценку для связок интуиционистского исчисления высказываний следующим образом:

$$\begin{aligned} \llbracket A \& B \rrbracket &= \llbracket A \rrbracket \cap \llbracket B \rrbracket \\ \llbracket A \vee B \rrbracket &= \llbracket A \rrbracket \cup \llbracket B \rrbracket \\ \llbracket A \rightarrow B \rrbracket &= (c[\llbracket A \rrbracket] \cup \llbracket B \rrbracket)^\circ \\ \llbracket \neg A \rrbracket &= (c[\llbracket A \rrbracket])^\circ \end{aligned}$$

Будем считать, что формула истинна в данной модели, если её значение оказалось равно всему пространству.

Например, возьмем в качестве пространства \mathbb{R} , и вычислим значение формулы $A \vee \neg A$ при A равном $(0, 1)$: $\llbracket A \vee \neg A \rrbracket = (0, 1) \cup \llbracket \neg A \rrbracket = (0, 1) \cup (c(0, 1))^\circ = (0, 1) \cup ((-\infty, 0) \cup (1, \infty)) = (-\infty, 0) \cup (0, 1) \cup (1, \infty)$. Нетрудно видеть, что данная формула оказалась не общезначимой в данной интерпретации.

5.2 Модели Крипке

См. Шень, Верещагин

6 Исчисление предикатов

Выберем множество истинностных значений V . Также, выберем некоторое предметное множество D . n -местным предикатом мы назовем функцию из D^n в V . Как и раньше, мы ограничимся классическим множеством V – истина и ложь, но оставляем потенциальную возможность его расширить.

Предикаты могут быть 0-местными, в этом случае это хорошо нам известные пропозициональные переменные, принимающие какие-то истинностные значения, в происхождение которых мы не вникаем.

Рассмотрим следующий известный пример: каждый человек смертен, Сократ - человек, следовательно, Сократ - смертен. Мы можем формализовать это выражение с помощью предикатов: множество D - это будет множество всех существ, $S(x)$ - предикат «быть смертным», $H(x)$ - предикат «быть человеком». Тогда фраза в полу-формальном виде выглядит так: Для каждого x , такого, что $H(x)$ верно $S(x)$, поэтому поскольку $H(\text{Сократ})$, значит, что имеет место $S(\text{Сократ})$.

Определим язык исчисления предикатов более точно. В исчислении предикатов появляется два типа значений: логические (которые участвуют в связках) и предметные (со значениями из множества D). Соответственно, все выражения также делятся на два типа.

Логические выражения — это логические связки плюс предикаты — обобщение пропозициональных переменных, которые теперь могут иметь параметрами предметные выражения.

Предметные выражения — это либо *предметные переменные* (обозначаются маленькими латинскими буквами, также возможно с индексами), либо *функции*, которые действуют из D^n в D .

Например, в выражении $1 + 5 = 0$, понимаемом в смысле исчисления предикатов, есть три константы (то есть, три нуль-местных функции — это 0, 1 и 5), одна двухместная функция (плюс), и один предикат (равенство).

Формула исчисления предикатов — это всегда логическое выражение. Например, $5 + 1$ в смысле предыдущего примера не может являться формулой исчисления предикатов.

Помимо этого, мы добавим две новых логических связки:

- Квантор всеобщности: $\forall x \alpha$ (здесь и в следующем определении x — некоторая предметная переменная, а α — некоторая формула исчисления предикатов).
- Квантор существования: $\exists x \alpha$.

Кванторы ведут себя как унарные операции и действуют только на ближайшее за ними выражение логического типа. Например, формула $\forall x x = 5 \vee x = 7$ соответствует формуле $(\forall x (x = 5)) \vee (x = 7)$.

Мы надеемся, что в целом смысл этих конструкций интуитивно понятен, теперь мы перейдем к более формальному описанию.

6.1 Доказательства в исчислении предикатов

Определение 6.1. Дана некоторая формула s . Будем говорить, что подстрока s_1 строки s является подформулой, если она в точности соответствует какому-то одному нетерминалу в дереве разбора строки s .

Определение 6.2. Если в формулу входит подформула, полученная по правилам для кванторов (то есть, $\forall x \alpha$ или $\exists x \alpha$), то мы будем говорить, что формула α находится в области действия данного квантора по переменной x . Также, будем говорить, что любая подформула формулы α находится в области действия данного квантора.

Определение 6.3. Если некоторое вхождение переменной x находится в области действия квантора по переменной x , то такое вхождение мы назовем *связанным*. Вхождение переменной x непосредственно рядом с квантором $(\forall x \dots)$ мы назовем *связывающим*. Те вхождения переменных, которые не являются связанными или связывающими, назовем *свободными*. Формула, не имеющая свободных вхождений переменных, называется *замкнутой*.

Определение 6.4. Будем говорить, что переменная y свободна для x при подстановке в формулу ψ (или просто свободна для подстановки вместо x), если после подстановки y вместо свободных вхождений x ни одно ее вхождение не станет связанным.

Чтобы получить список аксиом для исчисления предикатов, возьмем все схемы аксиом исчисления высказываний и дополним их следующими двумя схемами. Здесь x - переменная, ψ - некоторая формула, y - некоторая переменная. Запись $\psi[x := y]$ будет означать результат подстановки y в ψ вместо всех свободных вхождений x . Пусть y свободно для подстановки вместо x .

$$(11) \quad \forall x(\psi) \rightarrow (\psi[x := \alpha])$$

$$(12) \quad (\psi[x := \alpha]) \rightarrow \exists x(\psi)$$

Заметим, что если взять формулу $\exists x A(x, y)$, то по схеме аксиом (11), если игнорировать ограничение на свободу для подстановки, следующее утверждение должно быть тавтологией: $\forall y \exists x A(x, y) \rightarrow \exists x A(x, x)$. Однако, оно ей не является.

Все аксиомы, порожденные данными схемами в новом языке, мы назовем аксиомами исчисления предикатов.

Правила вывода. Пусть x не входит свободно в ϕ . Тогда рассмотрим следующие дополнительные правила вывода исчисления предикатов:

$$\frac{(\phi) \rightarrow (\psi)}{(\phi) \rightarrow \forall x(\psi)} \quad \frac{(\psi) \rightarrow (\phi)}{\exists x(\psi) \rightarrow (\phi)}$$

Добавив эти схемы к схеме для правила Modus ponens исчисления высказываний, мы сможем породить множество правил вывода.

6.2 Оценка выражений в исчислении предикатов

Для задания оценки для выражения в исчислении предикатов необходимо вместо оценки для переменных f_P в исчислении высказываний ввести оценку для предикатов: для каждого k -местного предиката P_n^k определить функцию $f_{P_n^k} : D^k \rightarrow V$.

Определение 6.5. Формула в исчислении предикатов общезначима, если она истинна на любом предметном множестве D , при любой оценке предикатов, и при любых оценках свободных индивидуальных переменных.

Определение 6.6. Пусть имеется некоторое исчисление предикатов с множеством аксиом A , и пусть дан некоторый (возможно, пустой) список Γ формул исчисления предикатов. Тогда, вывод формулы α в исчислении с аксиомами $A \cup \Gamma$ мы назовем выводом из допущений Γ , и будем записывать это как $\Gamma \vdash \alpha$.

Обратите внимание на требование отсутствия свободных переменных в допущениях.

Теорема 6.1. Исчисление предикатов корректно, т.е. любое доказуемое утверждение общезначимо.

Доказательство. Упражнение. □

Теорема 6.2. Теорема о дедукции. Если $\Gamma, \alpha \vdash \beta$, и в доказательстве отсутствуют применения правил для кванторов, использующих свободные переменные из формулы α , то $\Gamma \vdash \alpha \rightarrow \beta$

Доказательство. Доказательство разбором случаев. 3 старых случая те же, добавилось 2 новых правила вывода. Упражнение. □

Теорема 6.3. Исчисление предикатов полно.

Доказательство. Шень, Верещагин + Коэн. Будет добавлено позже. □

7 Теории первого порядка

Мы занимались до этого момента только логическими рассуждениями самими по себе. Это интересно, но не очень практически полезно: мы все-таки используем логические рассуждения для доказательства утверждений о каких-то объектах. Было бы разумно каким-то образом включить эти объекты в рамки формальной теории.

Рассмотрим некоторое множество N . Будем говорить, что оно удовлетворяет аксиомам Пеано, если выполнено следующее:

- В нем существует некоторый выделенный элемент 0 .
- Для каждого элемента множества определена операция $'$.

Кроме того, эти элемент и операция должны удовлетворять следующим требованиям:

- Не существует такого x , что $x' = 0$.
- Если $x' = y'$, то $x = y$.
- Если некоторое предположение верно для 0 , и если из допущения его для n можно вывести его истинность для $n + 1$, то предположение верно для любого элемента множества.

Данная аксиоматика позволяет определить натуральные числа (множество натуральных чисел — это множество, удовлетворяющее аксиомам Пеано; заметим, что тут натуральные числа содержат 0 , так оказывается удобнее) и операции над ними. Например, сложение можно задать следующими уравнениями:

$$\begin{aligned}a + 0 &= a \\ a + b' &= (a + b)'\end{aligned}$$

Теорема 7.1. Так определенное сложение коммутативно.

Доказательство. Упражнение. □

Но данная аксиоматика сформулирована неформально, поэтому мы не сможем доказать никаких содержательных утверждений про нее, пользуясь формальными средствами. Поэтому нам нужно эту конструкцию как-то объединить с исчислением предикатов, чем мы сейчас и займемся.

Возьмем язык исчисления предикатов со следующими изменениями и особенностями:

- Маленькими латинскими буквами a, b, \dots (возможно, с индексами) будем обозначать индивидуальные переменные.
- К логическим связкам добавляются такие: $(=)$ — двуместный предикат, $(+)$ и (\cdot) — двуместные функции, и $(')$ — одноместная функция. Все левоассоциативное, приоритеты в порядке убывания: $(')$, потом (\cdot) , потом $(+)$. Все логические связки имеют приоритет ниже. Например, $a = b' + b' + c \cdot c \& b = c$ надо интерпретировать как $(a = (((b') + (b')) + (c \cdot c))) \& (b = c)$.
- Вводится 0 -местная функция 0 .

К стандартным аксиомам исчисления предикатов добавим следующие 8 *нелогических* аксиом и одну нелогическую схему аксиом.

- (A1) $a = b \rightarrow a' = b'$
- (A2) $a = b \rightarrow a = c \rightarrow b = c$
- (A3) $a' = b' \rightarrow a = b$
- (A4) $\neg a' = 0$
- (A5) $a + b' = (a + b)'$
- (A6) $a + 0 = a$
- (A7) $a \cdot 0 = 0$
- (A8) $a \cdot b' = a \cdot b + a$
- (A9) $(\psi[x := 0]) \& \forall x((\psi) \rightarrow (\psi)[x := x']) \rightarrow (\psi)$

В схеме аксиом (A9) ψ — некоторая формула исчисления предикатов и x — некоторая переменная, входящая свободно в ψ .

Теорема 7.2. $\vdash a = a$

Доказательство. Упражнение. Клини, стр. 254. □

Определение 7.1. Структура. Структурой теории первого порядка мы назовем упорядоченную тройку $\langle D, F, P \rangle$, где $F = \langle F_0, F_1, \dots \rangle$ — списки оценок для 0-местных, 1-местных и т.д. функций, и $P = \langle P_0, P_1, \dots \rangle$ — списки оценок для 0-местных, 1-местных и т.д. предикатов, D — предметное множество.

Понятие структуры — развитие понятия оценки из исчисления предикатов. Но оно касается только нелогических составляющих теории; истинностные значения и оценки для связок по-прежнему определяются исчислением предикатов, лежащим в основе теории. Для получения оценки формулы нам нужно задать структуру, значения всех свободных индивидуальных переменных, и (естественным образом) вычислить результат.

Определение 7.2. Назовем структуру корректной, если любая доказуемая формула истинна в данной структуре.

Определение 7.3. Моделью теории мы назовем любую корректную структуру.

Еще одним примером теории первого порядка может являться теория групп. К исчислению предикатов добавим двуместный предикат $(=)$, двуместную функцию (\cdot) , одноместную функцию (x^{-1}) , константу (т.е. 0-местную функцию) 1 и следующие аксиомы:

- (E1) $a = b \rightarrow (a = c \rightarrow b = c)$
- (E2) $a = b \rightarrow (a \cdot c = b \cdot c)$
- (E3) $a = b \rightarrow (c \cdot a = c \cdot b)$
- (G1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- (G2) $a \cdot 1 = a$
- (G3) $a \cdot a^{-1} = 1$

Теорема 7.3. Доказуемо, что $a = b \rightarrow b = a$ и что $a^{-1} \cdot a = 1$.

Доказательство. Упражнение. □

8 Рекурсивные функции.

Рассмотрим примитивы, из которых будем собирать выражения:

1. $Z : N \rightarrow N$, $Z(x) = 0$
2. $N : N \rightarrow N$, $N(x) = x'$
3. Проекция. $U_i^n : N^n \rightarrow N$, $U_i^n(x_1, \dots, x_n) = x_i$
4. Подстановка. Если $f : N^n \rightarrow N$ и $g_1, \dots, g_n : N^m \rightarrow N$, то $S\langle f, g_1, \dots, g_n \rangle : N^m \rightarrow N$. При этом $S\langle f, g_1, \dots, g_n \rangle(x_1, \dots, x_m) = f(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m))$
5. Примитивная рекурсия. Если $f : N^n \rightarrow N$ и $g : N^{n+2} \rightarrow N$, то $R\langle f, g \rangle : N^{n+1} \rightarrow N$, при этом

$$R\langle f, g \rangle(x_1, \dots, x_n, y) = \begin{cases} f(x_1, \dots, x_n) & , y = 0 \\ g(x_1, \dots, x_n, y-1, R\langle f, g \rangle(x_1, \dots, x_n, y-1)) & , y > 0 \end{cases}$$

6. Минимизация. Если $f : N^{n+1} \rightarrow N$, то $\mu\langle f \rangle : N^n \rightarrow N$, при этом $\mu\langle f \rangle(x_1, \dots, x_n)$ — такое минимальное число y , что $f(x_1, \dots, x_n, y) = 0$. Если такого y нет, результат данного примитива неопределен.

Если некоторая функция $N^n \rightarrow N$ может быть задана с помощью данных примитивов, то она называется рекурсивной. Если некоторую функцию можно собрать исключительно из первых 5 примитивов (то есть без использования операции минимизации), то такая функция называется примитивно-рекурсивной.

Теорема 8.1. Следующие функции являются примитивно-рекурсивными: сложение, умножение, ограниченное вычитание (которое равно 0, если результат вычитания отрицателен), целочисленное деление, остаток от деления.

Доказательство. Упражнение. □

9 Арифметические функции и отношения. Их выразимость в формальной арифметике.

Введем обозначение. Если в тексте вводится некоторая формула $\alpha(x_1, \dots, x_n)$, то по умолчанию считается, что эта формула имеет минимум n свободных переменных, с именами x_1, \dots, x_n

Внутри же выражения запись $\alpha(y_1, \dots, y_n)$ мы будем трактовать, как $\alpha[x_1 := y_1, \dots, x_n := y_n]$, при этом мы подразумеваем, что y_1, \dots, y_n свободны для подстановки вместо x_1, \dots, x_n в α .

Также, запись $B(x_1, \dots, x_n) \equiv \alpha(x_1, \dots, x_n)$ будет означать, что мы определяем новую формулу с именем B и n свободными переменными x_1, \dots, x_n . Данная формула должна восприниматься только как сокращение записи, макроподстановка.

Определение 9.1. Арифметическая функция — функция $f : N^n \rightarrow N$. Арифметическое отношение — n -арное отношение, заданное на N .

Определение 9.2. Арифметическое отношение R называется выразимым (в формальной арифметике), если существует такая формула $\alpha(x_1, \dots, x_n)$ с n свободными переменными, что для любых натуральных чисел $k_1 \dots k_n$

1. если $(k_1, \dots, k_n) \in R$, то доказуемо $\alpha(\overline{k_1}, \dots, \overline{k_n})$
2. если $(k_1, \dots, k_n) \notin R$, то доказуемо $\neg\alpha(\overline{k_1}, \dots, \overline{k_n})$.

Например, отношение $(<)$ является выразимым в арифметике: Рассмотрим формулу $\alpha(a_1, a_2) = \exists b(\neg b = 0 \& a_1 + b = a_2)$. В самом деле, если взять некоторые числа k_1 и k_2 , такие, что $k_1 < k_2$, то найдется такое положительное число b , что $k_1 + b = k_2$. Можно показать, что если подставить $\overline{k_1}$ и $\overline{k_2}$ в α , то формула будет доказуема.

Наметим доказательство: Тут должно быть два доказательства по индукции, сперва по k_2 , потом по k_1 . Рассмотрим доказательство по индукции: пусть $k_1 = 0$, индукция по 2-му параметру: Разберем доказательство базы при $k_2 = 1$. Тогда надо показать $\exists b(\neg b = 0 \& 0 + b = 1)$:

- | | |
|--|------------------------|
| (1) $\neg 1 = 0 \& 0 + 1 = 1$ | Несложно показать |
| (2) $(\neg 1 = 0 \& 0 + 1 = 1) \rightarrow \exists b(\neg b = 0 \& 0 + b = 1)$ | Сх. акс. для \exists |
| (3) $\exists b(\neg b = 0 \& 0 + b = 1)$ | М.Р. 1 и 2. |

Определение 9.3. Введем следующее сокращение записи: пусть $\exists! y \phi(y)$ означает

$$\exists y \phi(y) \& \forall a \forall b (\phi(a) \& \phi(b) \rightarrow a = b)$$

Здесь a и b — некоторые переменные, не входящие в формулу ϕ свободно.

Определение 9.4. Арифметическая функция f от n аргументов называется представимой в формальной арифметике, если существует такая формула $\alpha(x_1, \dots, x_{n+1})$ с $n + 1$ свободными переменными, что для любых натуральных чисел $k_1 \dots k_{n+1}$

1. $f(k_1, \dots, k_n) = k_{n+1}$ тогда и только тогда, когда доказуемо $\alpha(\overline{k_1}, \dots, \overline{k_{n+1}})$.
2. Доказуемо $\exists! b(\alpha(\overline{k_1}, \dots, \overline{k_n}, b))$

Теорема 9.1. Функции Z , N , U_i^n являются представимыми.

Доказательство. Наметим доказательство. Для этого приведем формулы, доказательство корректности этих формул оставим в виде упражнения.

- Прimitив Z представит формула $Z(a, b) := (a = a \& b = 0)$.
- Прimitив N представит формула $N(a, b) := (a' = b)$.
- Прimitив U_i^n представит формула $U_i^n(a_1, \dots, a_n, b) = (a_1 = a_1) \& \dots \& (a_n = a_n) \& (b = a_i)$.

□

Теорема 9.2. Если функции f и g_1, \dots, g_m представимы, то функция $S\langle f, g_1, \dots, g_m \rangle$ также представима.

Доказательство. Поскольку функции f и g_i представимы, то есть формулы F и G_1, \dots, G_m , их представляющие. Тогда следующая формула представит $S\langle f, g_1, \dots, g_m \rangle$:

$$S(a_1, \dots, a_n, b) := \exists b_1 \dots \exists b_m (G_1(a_1, \dots, a_n, b_1) \& \dots \& G_m(a_1, \dots, a_n, b_m) \& F(b_1, \dots, b_m, b))$$

□

Определение 9.5. Характеристическая функция арифметического отношения R — это функция

$$C_R(x_1, \dots, x_n) = \begin{cases} 0 & R(x_1, \dots, x_n) \\ 1 & R(x_1, \dots, x_n) \text{ неверно} \end{cases}$$

Очевидно, что характеристическая функция представима тогда и только тогда, когда отношение выражимо.

Определение 9.6. β -функция Геделя - это функция $\beta(b, c, i) = b \% (1 + c \cdot (i + 1))$. Здесь операция $(\%)$ означает взятие остатка от целочисленного деления.

Лемма 9.3. Функция примитивно-рекурсивна, и при этом представима в арифметике формулой $B(b, c, i, d) := \exists q((b = q \cdot (1 + c \cdot (i + 1)) + d) \& (d < 1 + c \cdot (i + 1)))$

Доказательство. Упражнение. □

Лемма 9.4. Для любой конечной последовательности чисел $k_0 \dots k_n$ можно подобрать такие константы b и c , что $\beta(b, c, i) = k_i$ для $0 \leq i \leq n$.

Доказательство. Возьмем число $c = \max(k_1, \dots, k_n, n)!$. Рассмотрим числа $u_i = 1 + c \cdot (i + 1)$.

- Никакие числа u_i и u_j ($0 \leq j < i \leq n$) не имеют общих делителей кроме 1. Пусть это не так, и есть некоторый общий делитель p (очевидно, мы можем предположить его простоту — разложив на множители, если он составной). Тогда p будет делить $u_i - u_j = c \cdot (i - j)$, при этом p не может делить c — иначе окажется, что $u_i = (1 + c \cdot (i + 1))$ делится на p и $c \cdot (i + 1)$ делится на p . Значит, p делит $i - j$, то есть все равно делит c , так как c — факториал некоторого числа, не меньшего n , и при этом $i - j \leq n$.
- Каждое из чисел k_i меньше, чем u_i : в самом деле, $k_i \leq c < 1 + c \cdot (i + 1) = u_i$.
- Согласно китайской теореме об остатках, если некоторые натуральные числа k_0, \dots, k_n попарно взаимно просты, то для любых целых чисел u_0, \dots, u_n , таких, что $0 \leq k_i < u_i$, найдется такое целое число b , для которого выполнено $k_i = b \% u_i$. Возьмем b , подсказываемое теоремой об остатках.

□

Теорема 9.5. Всякая рекурсивная функция представима в арифметике.

Доказательство. Представимость первых четырех примитивов уже показана. Покажем представимость примитивной рекурсии и операции минимизации.

Примитивная рекурсия. Пусть есть некоторый $R\langle f, g \rangle$. Соответственно, f и g уже представлены как некоторые формулы F и G . Из определения $R\langle f, g \rangle$ мы знаем, что для значения $R\langle f, g \rangle(x_1, \dots, x_{n+1})$ должна существовать последовательность $a_0 \dots a_{x_{n+1}}$ результатов применения функций f и g — значений на одно больше, чем итераций в цикле примитивной рекурсии, а это количество определяется последним параметром функции $R\langle f, g \rangle$. При этом:

$$\begin{aligned} a_0 &= f(x_1, \dots, x_n) \\ a_1 &= g(x_1, \dots, x_n, 0, a_0) \\ &\dots \\ a_{x_{n+1}} &= g(x_1, \dots, x_n, x_{n+1} - 1, a_{x_{n+1}-1}) \end{aligned}$$

Значит, по лемме, должны существовать такие числа b и c , что $\beta(b, c, i) = a_i$ для $0 \leq i \leq x_{n+1}$.

Приведенные рассуждения позволяют построить следующую формулу, представляющую $R\langle f, g \rangle(x_1, \dots, x_{n+1})$:

$$\begin{aligned} R(x_1, \dots, x_{n+1}, a) &:= \exists b \exists c (\exists k (B(b, c, 0, k) \& F(x_1, \dots, x_n, k)) \\ &\quad \& B(b, c, x_{n+1}, a) \\ &\quad \& \forall k (k < x_{n+1} \rightarrow \exists d \exists e (B(b, c, k, d) \& B(b, c, k', e) \& G(x_1, \dots, x_n, k, d, e))) \end{aligned}$$

Минимизация. Рассмотрим конструкцию $\mu\langle f \rangle$. f уже представлено как некоторая формула F . Тогда формула $M(x_1, \dots, x_n, y) := F(x_1, \dots, x_n, y, 0) \& \forall z (z < y \rightarrow \neg F(x_1, \dots, x_n, z, 0))$ представит $\mu\langle f \rangle$.

□

10 Гёделева нумерация. Арифметизация доказательств

Ранее мы показали, что любое рекурсивное арифметическое отношение выразимо в формальной арифметике. Теперь мы покажем, что любое выражимое в формальной арифметике отношение является рекурсивным.

Определение 10.1. Ограниченные кванторы $\exists_{x < y} \phi(x)$ и $\forall_{x < y} \phi(x)$ — сокращения записи для выражений вида $\exists x(x < y \& \phi(x))$ и $\forall x(x \geq y \vee \phi(x))$

Теорема 10.1. Пусть P_1 и P_2 — рекурсивные отношения. Тогда следующие формулы, задающие некоторые отношения, также являются рекурсивными отношениями:

1. $F(x_1, \dots, x_n, z) := \forall_{y < z} P_1(x_1, \dots, x_n, y)$
2. $E(x_1, \dots, x_n, z) := \exists_{y < z} P_1(x_1, \dots, x_n, y)$
3. $P_1(x_1, \dots, x_n) \rightarrow P_2(x_1, \dots, x_n)$
4. $P_1(x_1, \dots, x_n) \vee P_2(x_1, \dots, x_n)$
5. $P_1(x_1, \dots, x_n) \& P_2(x_1, \dots, x_n)$
6. $\neg P_1(x_1, \dots, x_n)$

Доказательство. Упражнение. □

Теперь мы перенесем понятие вывода формулы на язык рекурсивных отношений, и, следовательно, внутрь языка формальной арифметики.

Определение 10.2. Гёделева нумерация. Дадим следующие номера символам языка формальной арифметики:

3	(
5)	
7	,	
9	\neg	
11	\rightarrow	
13	\vee	
15	$\&$	
17	\forall	
19	\exists	
$13 + 8 \cdot k$	x_k	переменные
$15 + 8 \cdot k$	a_k	константы
$17 + 8 \cdot 2^k \cdot 3^n$	f_k^n	n-местные функциональные символы: $()$, $(+)$ и т.п.
$19 + 8 \cdot 2^k \cdot 3^n$	P_k^n	n-местные предикаты, в т.ч. $(=)$

Уточним язык — обяжем всегда писать скобки всегда и только вокруг двуместной операции. В принципе, иначе мы могли бы определить правильно операцию равенства E_q , но это лишние технические сложности.

Научимся записывать выражения в виде чисел. Пусть p_1, \dots, p_k, \dots — список простых чисел, при этом $p_1 = 2, p_2 = 3, \dots$

Тогда текст из n символов с гёделевыми номерами c_1, \dots, c_n запишем как число $t = p_1^{c_1} \cdot p_2^{c_2} \cdot \dots \cdot p_n^{c_n}$. Ясно, что такое представление однозначно позволяет установить длину строки (гёделева нумерация не содержит 0, поэтому можно определить длину строки как

максимальный номер простого числа, на которое делится t ; будем записывать эту функцию как $Len(s)$, и каждый символ строки в отдельности (будем записывать функцию как $(s)_n$). Также ясно, что функции Len и $(x)_n$ — рекурсивны.

Чтобы удобнее работать со строками, введем следующие обозначения, за которыми скрываются рекурсивные функции:

- запись « $c_1 c_2 c_3 \dots$ » (где c_i — какие-то символы языка формальной арифметики) задаёт рекурсивную функцию, игнорирующую свои аргументы, и возвращающую число $p_1^{c_1} \cdot \dots \cdot p_n^{c_n}$.
- Операцию конкатенации строк определим так. Пусть S и T — рекурсивные функции, результат вычисления которых являются числа $s = p_1^{s_1} \cdot \dots \cdot p_n^{s_n}$ и $t = p_1^{t_1} \cdot \dots \cdot p_m^{t_m}$ соответственно. Тогда $S@T$ — это рекурсивная функция, вычисляющая функции S и T , результатом работы которой будет $p_1^{s_1} \cdot \dots \cdot p_n^{s_n} \cdot p_{n+1}^{t_1} \cdot \dots \cdot p_{n+m}^{t_m}$.
- Внутри кавычек мы вводим операцию подстановки переменных. Если внутри кавычек указан символ доллара ($\$$), то следующий за ним символ должен интерпретироваться как имя аргумента функции, при этом значение кавычек должно вычисляться как конкатенация строки до этого аргумента, значения самого аргумента, и строки после аргумента: « $\dots \$x \dots$ » = « \dots »@ U_x^n @« \dots ».

Чтобы представить доказательства, мы будем объединять строки вместе так же, как объединяем символы в строки: $2^{2^3} \cdot 3^{2^5}$ — это последовательность из двух строк, первая — это «(», а вторая — «)».

Теперь мы можем понять, как написать программу, проверяющую корректность доказательства некоторого утверждения в формальной арифметике. Наметим общую идею. Программа будет состоять из набора рекурсивных отношений и функций, каждое из которых выражает некоторое отношение, содержательное для проверки доказательства. Ниже мы покажем идею данной конструкции, приведя несколько из них.

- Проверка того, что a — гёделев номер выражения, являющегося переменной. $Var(a) \equiv \exists z < a (a = 2^{13+z})$
- Проверка того, что выражение с номером a получено из выражений b и c путем применения правила Modus Ponens. $MP(b, c, a) \equiv c = «(\$b \rightarrow \$a)»$
- Проверка того, что b получается из a подстановкой y вместо x : $Subst(a, b, x, y)$ — без реализации
- Функция, подставляющая y вместо x в формуле a :
 $Sub(a, x, y) \equiv \mu \langle S \langle Subst, U_1^4, U_4^4, U_2^4, U_3^4 \rangle \rangle (a, x, y)$
- Проверка того, что переменная x входит свободно в формулу f .
 $Free(f, x) \equiv \neg Subst(a, a, x, 13 + 8^x)$
- Функция, выдающая гёделев номер выражения, соответствующего целому числу:
 $Num(n) \equiv R \langle «0», U_3^3 @ «'» \rangle (n, n)$

Путем некоторых усилий мы можем выписать формулу, представляющую двуместное отношение $Proof(f, p)$, истинное тогда и только тогда, когда p — гёделев номер доказательства формулы с гёделевым номером f .

Теорема 10.2. Любая представимая в формальной арифметике функция является рекурсивной.

Доказательство. Возьмем некоторую представимую функцию $f : N^n \rightarrow N$. Значит, для нее существует формула формальной арифметики, представляющая ее. Пусть F — эта формула (со свободными переменными x_1, \dots, x_n, y); при этом в случае $f(u_1, \dots, u_n) = v$ должно быть доказуемо $F(\overline{u_1}, \dots, \overline{u_n}, \overline{v})$. По формуле можно построить рекурсивную функцию, $C_F(u_1, \dots, u_n, v, p)$, выражающую тот факт, что p — гёделев номер вывода формулы $F(\overline{u_1}, \dots, \overline{u_n}, \overline{v})$. Тогда возьмем

$$f(x_1, \dots, x_n) \equiv (\mu \langle S \langle C_F, U_1^{n+1}, \dots, U_n^{n+1}, (U_{n+1}^{n+1})_1, (U_{n+1}^{n+1})_2 \rangle \rangle (x_1, \dots, x_n))_1$$

. □

11 1я и 2я теоремы Гёделя о неполноте арифметики

Определение 11.1. Мы будем называть теорию непротиворечивой, если не найдется такой формулы F , что доказуемо как F , так и $\neg F$.

Лемма 11.1. Если теория противоречива, то в ней доказуема любая формула.

Доказательство. Если теория противоречива, то в ней есть утверждение F , что доказуемо F и $\neg F$. Воспользуемся доказуемой формулой $\neg F \rightarrow F \rightarrow \beta$. \square

Определение 11.2. Мы будем называть теорию ω -непротиворечивой, если, какова бы ни была формула $P(x)$ со свободной переменной x , такая, что для любого натурального числа p доказуемо $P(\bar{p})$, то формула $\exists p \neg P(p)$ недоказуема.

Лемма 11.2. ω -непротиворечивость влечёт непротиворечивость.

Доказательство. Рассмотрим выводимую формулу $x = x \rightarrow x = x$. При подстановке любого натурального числа вместо x формула будет по-прежнему выводима: $\bar{k} = \bar{k} \rightarrow \bar{k} = \bar{k}$. Значит, по ω -непротиворечивости формула $\exists p \neg(x = x \rightarrow x = x)$ невыводима. Значит, теория непротиворечива (поскольку в противоречивой теории выводится любая формула). \square

Определим рекурсивное отношение $W_1(x, p)$, истинное тогда и только тогда, когда x есть гёделев номер формулы ϕ с единственным свободным аргументом x , а p есть гёделев номер доказательства $\phi(\ulcorner \phi \urcorner)$ — доказательства самоприменения ϕ . Это соотношение при достаточном развитии аппарата работы с доказательствами несложно выразить в формальной арифметике:

$$\omega_1(x, p) \equiv \text{Free}(x, \langle \mathbf{x} \rangle) \& \text{Proof}(\text{Sub}(x, \langle \mathbf{x} \rangle, \text{Num}(x)), p)$$

Заметим, что данное отношение является выразимым в формальной арифметике.

Рассмотрим формулу $\sigma \equiv \forall p \neg \omega_1(x, p)$ — это некоторая формула с единственной свободной переменной x , и посмотрим, что произойдёт с её самоприменением: $\sigma(\ulcorner \sigma \urcorner)$. Внимательное наблюдение за происходящим даст следующую теорему.

Теорема 11.3. Первая теорема Гёделя о неполноте арифметики.

1. Если формальная арифметика непротиворечива, то недоказуемо $\sigma(\ulcorner \sigma \urcorner)$.
2. Если формальная арифметика ω -непротиворечива, то недоказуемо $\neg \sigma(\ulcorner \sigma \urcorner)$.

Доказательство. 1. Пусть $\vdash \sigma(\ulcorner \sigma \urcorner)$. Тогда найдется гёделев номер ее доказательства p , значит, $W_1(\ulcorner \sigma \urcorner, p)$, то есть $\vdash \omega_1(\ulcorner \sigma \urcorner, \bar{p})$. С другой стороны, пользуясь схемой аксиом для квантора всеобщности и правилом Modus Ponens, из предположения теоремы $\vdash \sigma(\ulcorner \sigma \urcorner)$ (то есть $\vdash \forall p \neg \omega_1(\ulcorner \sigma \urcorner, p)$) можно показать $\vdash \neg \omega_1(\ulcorner \sigma \urcorner, \bar{p})$. Противоречие.

2. Пусть $\vdash \neg \sigma(\ulcorner \sigma \urcorner)$, то есть $\vdash \neg \forall p \neg \omega_1(\ulcorner \sigma \urcorner, p)$, то есть $\vdash \exists p \omega_1(\ulcorner \sigma \urcorner, p)$. Значит, неизбежно найдется такой номер q , что $\vdash \omega_1(\ulcorner \sigma \urcorner, \bar{q})$, поскольку если бы для каждого q было бы доказуемо $\vdash \neg \omega_1(\ulcorner \sigma \urcorner, \bar{q})$, то по ω -непротиворечивости было бы недоказуемо $\exists p \neg \omega_1(\ulcorner \sigma \urcorner, p)$.

Рассмотрев же определение W_1 , можно заметить, что найденный q также есть номер доказательства $\sigma(\ulcorner \sigma \urcorner)$, что вступает в противоречие с предположением $\vdash \neg \sigma(\ulcorner \sigma \urcorner)$. \square

Формула $\sigma(\ulcorner \sigma \urcorner)$, говоря простым языком, утверждает собственную недоказуемость. Мы показали, что эта формула (при условии ω -непротиворечивости формальной арифметики) действительно недоказуема — что означает её общезначимость. Таким образом, мы показали, что если формальная арифметика ω -непротиворечива, то она неполна.

В данном рассуждении используется сложное понятие ω -непротиворечивости, что смущает. Теорема Гёделя в форме Россера снимает эту сложность.

Рассмотрим отношение $W_2(x, p) \rightarrow x$ и p состоят в отношении W_2 тогда и только тогда, когда p - гёделев номер доказательства отрицания самоприменения x (если ϕ — формула от одной переменной x , то p — номер доказательства $\neg\phi(\ulcorner\phi\urcorner)$). Мы также можем выразить его в формальной арифметике аналогично ω_1 (обозначим представляющую формулу за ω_2).

Тогда рассмотрим формулу $\rho(x) \equiv \forall p(\omega_1(x, p) \rightarrow \exists q(q < p \& \omega_2(x, q)))$. Неформальным языком она утверждает, что для любого доказательства самоприменения некоторой формулы с номером a найдется доказательство (да еще и с меньшим гёделевым номером) отрицания этой формулы. Ну и по традиции применим ее к своему номеру r . Внимательное рассмотрение этой ситуации приводит к следующей теореме.

Теорема 11.4. Теорема Гёделя в форме Россера. Если формальная арифметика непротиворечива, то найдется такая формула ϕ , что как она сама, так и ее отрицание недоказуемы.

Доказательство. В качестве формулы ϕ возьмем формулу $\rho(\ulcorner\rho\urcorner)$.

Покажем недоказуемость ϕ . Пусть $\vdash \rho(\ulcorner\rho\urcorner)$, т.е. $\forall p(\omega_1(\ulcorner\rho\urcorner, p) \rightarrow \exists q(q < p \& \omega_2(\ulcorner\rho\urcorner, q)))$ истинно. Значит, есть такой p , что $\exists q(q < p \& \omega_2(\ulcorner\rho\urcorner, q))$ истинно. Значит, найдется такой $q < p$, что $W_2(\ulcorner\rho\urcorner, q)$ истинно, т.е., что q — номер опровержения ϕ , что влечёт за собой противоречивость арифметики.

Обратно, пусть $\vdash \neg\phi$. Пусть t - гёделев номер доказательства. Раз так, то $W_2(\ulcorner\rho\urcorner, t)$ истинно. По непротиворечивости формальной арифметики это значит, что $W_1(\ulcorner\rho\urcorner, p)$ при любом p ложно (иначе окажется, что найдутся как доказательство, так и опровержение $\rho(\ulcorner\rho\urcorner)$). Значит, доказуемо $\neg\omega_1(\ulcorner\rho\urcorner, \bar{p})$ при любом p (т.е. никакой из p не является доказательством $\rho(\ulcorner\rho\urcorner)$). Как частный случай, $\neg\omega_1(\ulcorner\rho\urcorner, \bar{x})$ доказуемо для всех x , не превышающих t , поэтому $\vdash \neg\omega_1(\ulcorner\rho\urcorner, \bar{0}) \& \neg\omega_1(\ulcorner\rho\urcorner, \bar{1}) \& \dots \& \neg\omega_1(\ulcorner\rho\urcorner, \bar{t})$. Отсюда можно показать $\vdash p \leq \bar{t} \rightarrow \neg\omega_1(\ulcorner\rho\urcorner, p)$.

Рассмотрим формулу $(p > \bar{t}) \rightarrow \exists q(q < p \& \omega_2(\ulcorner\rho\urcorner, q))$. Формула утверждает следующее: «если некоторый p больше t , то найдется такой q , меньший p , что $W_2(\ulcorner\rho\urcorner, q)$ ». Очевидно, что данная формула истинна, ведь если мы возьмем t в качестве такого q , то $W_2(\ulcorner\rho\urcorner, t)$ истинно по предположению. В силу выразимости W_2 в формальной арифметике формула также и доказуема.

Легко показать, что из этих утверждений и из того, что $p \leq \bar{t} \vee p > \bar{t}$, можно вывести $\neg\omega_1(\ulcorner\rho\urcorner, p) \vee \exists q(q < p \& \omega_2(\ulcorner\rho\urcorner, q))$, а отсюда - $\forall p(\omega_1(\ulcorner\rho\urcorner, p) \rightarrow \exists q(q < p \& \omega_2(\ulcorner\rho\urcorner, q)))$, то есть ϕ . Однако, мы предположили доказуемость $\neg\phi$, и исходя из него, вывели ϕ , т.е. показали противоречивость формальной арифметики. Значит, $\neg\phi$ также недоказуемо, если арифметика непротиворечива. \square

Теорема 11.5. Вторая теорема Гёделя о неполноте арифметики. Если в формальной арифметике удастся доказать её непротиворечивость, то из этого доказательства можно построить доказательство её противоречивости.

Доказательство. Рассмотрим только схему доказательства. Возьмем *Consis*, некоторое утверждение, которое показывает непротиворечивость арифметики, т.е. показывает отсутствие такой формулы ϕ , что и ϕ и $\neg\phi$ доказуемы:

$$Consis \equiv \forall s((\forall p \neg Proof(s, p)) \vee (\forall p \neg Proof(\ulcorner\neg\urcorner@s, p)))$$

Тогда рассмотрим формулу $Consis \rightarrow \sigma(\ulcorner\sigma\urcorner)$. Данная формула в точности соответствует условию первой части первой теоремы Гёделя о неполноте арифметики (если арифметика непротиворечива, то самоприменение формулы σ недоказуемо; напомним, что $\sigma \equiv \forall p \neg\omega_1(x, p)$).

Рассуждение, доказывающее теорему Гёделя, можно формализовать, получив доказательство данной импликации. Теперь, если у нас будет доказательство утверждения

Consis, то по правилу Modus Ponens мы также получаем доказательство утверждения $\sigma(\overline{\Gamma\sigma\overline{}})$. Однако, существование такого доказательства влечет за собой противоречивость формальной арифметики. \square

Таким образом, внутри формальной арифметики нет способа доказать её непротиворечивость. Однако, можно пытаться это делать, находясь вне теории — используя более мощные формализмы. Например, Генцен доказал непротиворечивость арифметики, используя трансфинитную индукцию.

Последним в данном разделе заметим, что данные доказательства естественно обобщаются на случай произвольной формальной теории, включающей формальную арифметику. Достаточно только расширить правила, проверяющие доказательства формул на корректность (т.е. добавить в них новые аксиомы, схемы аксиом, и правила или схемы правил вывода).

12 Теория множеств.

Теория множеств — это еще одна теория первого порядка, с которой мы познакомимся в этом курсе. Мы добавим к исчислению предикатов один новый двуместный предикат — отношение принадлежности \in .

Для изучения теории множеств мы введем несколько сокращений записи. Первое сокращение — это новая логическая связка *эквивалентность*.

Определение 12.1. Эквивалентность. Запись $a \leftrightarrow b$ является сокращением записи для $\equiv a \rightarrow b \& b \rightarrow a$.

Определение 12.2. Будем говорить, что множество x является подмножеством множества y , если любой элемент x принадлежит y . Формально: $x \subseteq y$ является сокращением записи для $\forall z(z \in x \rightarrow z \in y)$.

Определение 12.3. Принцип объемности. Два множества называются равными, если они являются подмножествами друг друга. Формально: $x = y$ является сокращением записи для $x \subseteq y \& y \subseteq x$.

Аксиома 12.1. Аксиома равенства. Равные множества содержатся в одних и тех же множествах. $\forall x \forall y \forall z (x = y \& x \in z \rightarrow y \in z)$.

Аксиома 12.2. Аксиома пары. Каковы бы ни были два различных множества x и y , существует множество, состоящее в точности из них. Будем записывать его так: $\{x, y\}$. Формально: $\forall x \forall y (\neg x = y \rightarrow \exists p (x \in p \& y \in p \& \forall z (z \in p \rightarrow (z = x \vee z = y))))$.

Аксиома 12.3. Аксиома объединения. Для любого множества x , содержащего хотя бы один элемент, найдется такое множество, которое состоит в точности из тех элементов, из которых состоят элементы x . Будем записывать его так: $\cup x$. Формально: $\forall x (\exists y y \in x \rightarrow \exists p \forall y (y \in p \leftrightarrow \exists s (y \in s \& s \in x)))$

Аксиома 12.4. Аксиома степени. Каково бы ни было множество x , существует множество 2^x , содержащее в точности все возможные подмножества множества x . Формально: $\forall x \exists p \forall y (y \subseteq p \leftrightarrow y \in x)$.

Аксиома 12.5. Схема аксиом выделения. Для любого множества x и любой формулы от одного аргумента $\phi(y)$, такой, что b в нее не входит свободно, найдется такое множество b , в которое входят те и только те элементы из множества x , что $\phi(y)$ истинно. Формально: $\forall x \exists b \forall y (y \in b \leftrightarrow (y \in x \& \phi(y)))$

Определение 12.4. Пересечением множеств x и y называется множество, состоящее в точности из тех элементов, которые присутствуют и в x и в y . Формально: $x \cap y$ — это такое множество z , что $\forall t (t \in z \leftrightarrow t \in x \& t \in y)$

Определение 12.5. Пустое множество \emptyset — множество, которому не принадлежит никакой элемент: $\forall x \neg x \in \emptyset$.

Теорема 12.1. 1. Для любого множества X существует множество $\{X\}$, содержащее в точности X .

2. Если существует хотя бы одно множество, то существует пустое множество.

3. Пустое множество единственно.

4. Для двух множеств существует множество, являющееся их пересечением.

Определение 12.6. Дизъюнктным (разделённым) множеством называется множество, элементы которого не пересекаются. Формально: x дизъюнктно, если $\forall y \forall z (y \in x \& z \in x \rightarrow y = z)$.

Определение 12.7. Прямым произведением дизъюнктного множества a называется множество $\times a$ всех таких множеств b , что b пересекается с каждым из элементов множества a в точности в одном элементе.

$$\forall b (b \in \times a \leftrightarrow (\forall y (y \in a \rightarrow \exists! x (x \in y \& x \in b))))$$

Аксиома 12.6. Аксиома выбора. Прямое произведение непустого дизъюнктного множества, не содержащего пустых элементов, непусто. Формально: упражнение.

Аксиома 12.7. Аксиома бесконечности Существует множество N , такое, что:

$$\emptyset \in N \& \forall x (x \in N \rightarrow x \cup \{x\} \in N)$$

Аксиома 12.8. Аксиома фундирования В каждом непустом множестве найдется элемент, не пересекающийся с исходным множеством.

$$\forall x (x = \emptyset \vee \exists y (y \in x \& y \cap x = \emptyset))$$

Аксиома фундирования исключает множества, которые могут принадлежать сами себе (возможно, через цепочку принадлежностей): $X \in Y \in Z \in X$

Аксиома 12.9. Схема аксиом подстановки Если задана некоторая функция f , представляемая в исчислении предикатов (то есть, задан некоторый предикат A , такой, что $f(x) = y$ тогда и только тогда, когда $A(x, y) \& \exists! z A(x, z)$) то для любого множества Y существует множество $f(Y)$ — образ множества Y при отображении f .

Формально:

Ясно, что данная аксиома перекрывает аксиому выделения. Наличие аксиомы подстановки отличает аксиоматику Цермело-Френкеля от аксиоматики Цермело. Однако, ак

Определение 12.8. Упорядоченная пара Упорядоченной парой двух множеств a и b назовем множество $\{a, \{a, b\}\}$, еще будем записывать его так: $\langle a, b \rangle$

Лемма 12.2. Упорядоченную пару можно построить для любых множеств, также $\langle a, b \rangle = \langle c, d \rangle$ тогда и только тогда, когда $a = b$ и $c = d$.

Определение 12.9. Бинарное отношение Бинарным отношением на множестве X назовем подмножество множества всех упорядоченных пар элементов из X .

На бинарных отношениях естественным образом вводятся отношения рефлексивности, симметричности и транзитивности.

Определение 12.10. Упорядочивание Отношение R на множестве S упорядочивает X , если это отношение транзитивно и оно образует линейный порядок (строгое неравенство: справедливо $\forall x \forall y (x \in X \rightarrow y \in X \rightarrow R(x, y) \vee x = y \vee R(y, x))$ и $\forall x \neg R(x, x)$). Отношение вполне упорядочивает S , если к тому же для любого непустого подмножества S выполнено $\exists x (x \in B \& \forall y (y \in B \rightarrow \neg R(y, x)))$.

Также можно ввести понятие максимума, минимума, верхней грани, супремума.

Определение 12.11. Множество x - транзитивное, если $z \in y, y \in x \rightarrow z \in x$.

Определение 12.12. Ординал (порядковое число) — транзитивное, вполне упорядоченное с помощью отношения (\in) множество.

Рассмотрим ординалы подробнее. Для начала рассмотрим *конечные* ординалы: $0 := \emptyset$; $1 := \{\emptyset\}$; $2 := 1 \cup \{1\}$ и т.п. Существование каждого из этих ординалов легко доказать.

Определение 12.13. Ординал x называется предельным, если $\neg x = \emptyset \& \neg \exists y(y \cup \{y\} = x)$.

Минимальный предельный ординал мы обозначим ω . Ясно, что любое натуральное число меньше, чем ω . Также легко заметить, что ω содержит в себе в точности все конечные ординалы.

Для ординалов можно определить арифметические операции. В силу ограниченности курса мы сделаем это неформально, на мета-языке.

Определение 12.14. Арифметические операции над ординалами. За $a + 1$ обозначим $a \cup \{a\}$. Тогда следующими рекурсивными определениями мы введем операции сложения, умножения и возведения в степень:

$$\begin{aligned} a + b &\equiv \begin{cases} a, & b \equiv 0 \\ (a + c) + 1, & b \equiv c + 1 \\ \sup\{a + c \mid c < b\}, & b \text{ — предельный ординал} \end{cases} \\ a \cdot b &\equiv \begin{cases} 0, & b \equiv 0 \\ (a \cdot c) + a, & b \equiv c + 1 \\ \sup\{a \cdot c \mid c < b\}, & b \text{ — предельный ординал} \end{cases} \\ a^b &\equiv \begin{cases} 1, & b \equiv 0 \& a > 0 \\ (a^c) \cdot a, & b \equiv c + 1 \\ \sup\{a^c \mid c < b\}, & b \text{ — предельный ординал} \end{cases} \end{aligned}$$

Заметим, что в смысле введенной операции прибавления единицы, предельный ординал — это такой ненулевой ординал x , для которого нет ни одного ординала y , что $y + 1 = x$.

Так определенные операции на конечных ординальных числах ведут себя подобно обычным арифметическим операциям на натуральных числах, однако в целом их поведение может быть неочевидным. Например, легко заметить, что $1 + \omega = \omega$.

Определение 12.15. Назовем множества X и Y равномощными, если найдется биективное отображение X на Y . Будем записывать это как $|X| = |Y|$. Будем говорить, что множество X имеет мощность не превышающую Y , если найдется инъективное отображение X в Y . Будем записывать это как $|X| \leq |Y|$. Будем записывать $|X| < |Y|$, если известно, что $|X| \leq |Y|$, но неверно, что $|X| = |Y|$.

Определение 12.16. Кардинальные числа Кардинальное число — такой ординал x , что $y < x \leftrightarrow |y| < |x|$.

Ясно, что все конечные ординальные числа являются кардинальными. Также, например ω — кардинальное число (еще оно обозначается как \aleph_0 , если речь идет о мощности множеств). 2^ω — кардинальное число \aleph_1 , соответствует мощности континуум.

Есть ли какое-нибудь кардинальное число между \aleph_0 и \aleph_1 ? Континуум-гипотеза (что никаких других кардинальных чисел между ними нет) была высказана довольно давно, и длительное время была одной из главных проблем в теории множеств. Сначала Геделем было показано, что континуум-гипотеза не противоречит ZF. Утверждение о том, что и отрицание континуум-гипотезы не противоречит ZF, было доказано через 30 лет Коэном.

13 Теорема Лёвенгейма-Сколема

Как мы знаем из предыдущих разделов, рассмотрение формальной теории неполно, если не сопровождается рассмотрением её моделей. Действительно, каковы могут быть модели теории множеств? Например, обязан ли объект, соответствующий множеству мощности \aleph_1 действительно иметь несчётное количество элементов? В данном разделе мы прольём некоторый свет на этот вопрос.

Определение 13.1. Мощность модели. Пусть M — модель некоторой теории первого порядка. Напомним, что модель задаётся предметным множеством D , и функциями, соответствующим всем предикатам теории и всем функциональным символам теории. Тогда, назовем мощность множества D мощностью модели.

Определение 13.2. Элементарная подмодель. Пусть M — модель некоторой теории первого порядка, с предметным множеством D , и пусть определено D_1 , $D_1 \subset D$. Тогда структура M_1 , построенная на предметном множестве D_1 с предикатами и функциями, получающимися из предикатов и функций M путем сужения их области определения на D_1 называется *элементарной подмоделью* M , если:

1. любая функция теории f замкнута на D_1 (т.е. если $x_1 \in D_1, \dots, x_n \in D_1$, то $f(x_1, \dots, x_n) \in D_1$)
2. любая формула $A(x_1, \dots, x_n)$ теории при любых значениях x_1, \dots, x_n из M_1 истинна в M_1 тогда и только тогда, когда она истинна в M .

Заметим, что второе условие необходимо: пусть некоторая теория 1го порядка содержит предикат равенства. Тогда формула $\exists x \exists y \neg(x = y)$ при сужении предметного множества до одноэлементного перестаёт быть верной.

Лемма 13.1. Элементарная подмодель теории является моделью данной теории.

Доказательство. Рассмотрим некоторую доказуемую формулу теории A . Она является общезначимой в M , значит, она является общезначимой в M_1 . \square

Определение 13.3. Назовём теорию счётно-аксиоматизируемой (конечно-аксиоматизируемой), если ее множество аксиом и правил вывода имеет счётную (конечную) мощность.

Заметим, что количество аксиом определяет количество формул в теории. Можно создать теорию, в которой определены дополнительные функции и предикаты, ни разу не упоминаемые в аксиомах и правилах вывода, но такие «несодержательные» предикаты и функции не имеют смысла, поскольку мы можем приписать им любое значение (например, все функции выдают некоторую заранее выбранную константу c_0 , а все предикаты ложны), не повредив корректности модели. Поэтому в следующей теореме мы ограничимся рассмотрением мощности множества всех формул теории, заметив, что любая счётно-(конечно-)аксиоматизируемая теория будет иметь счётное (конечное) количество «содержательных» формул.

Теорема 13.2. Теорема Лёвенгейма-Сколема. Пусть M — модель некоторой теории первого порядка, и пусть T — множество всех возможных формул этой теории. Тогда у M есть элементарная подмодель, такая, что $|M| = \max(|T|, \aleph_0)$.

Доказательство. Для построения требуемой модели нам необходимо построить предметное множество требуемой мощности и показать, что сужение теории на него даст нам элементарную подмодель. Отсюда доказательство естественным образом разбивается на две части.

Часть 1. Построение множества. Рассмотрим некоторое предметное множество D' . На его основе построим множество D'' , рассмотрев все формулы из T , и по каждой формуле (возможно) добавив некоторое количество элементов к D' .

Фиксируем некоторую n -местную формулу $A(y, x_1, \dots, x_n)$ из T . Фиксируем некоторый набор аргументов x_1, \dots, x_n из D' . В ходе вычисления A в результате применения функций к аргументам мы можем выйти из D' — добавим эти новые константы к D'' . Их будет не более чем конечное количество. Заметим, что формула A может быть:

- тождественно истинной или ложной при любом y из D — пропустим эту формулу и пойдем дальше. Поступим так же, если функция может быть как истинной так и ложной при разных значениях y из D' .
- Найдутся такие y , что $A(y, x_1, \dots, x_n)$ истинна, но при этом для любого y из D' формула $A(y, x_1, \dots, x_n)$ ложна — тогда добавим какой-нибудь один из этих y к множеству D'' . Также пополним множество всеми константами, которые необходимо добавить вследствие вычисления A на данных аргументах. Этим мы также увеличим D'' на конечное количество элементов.

Рассмотрим множество D_0 , $D_0 \subseteq D$, такое, что в него входят только те элементы предметного множества, которые соответствуют константам (т.е. нуль-местным функциям), упоминающимся в формулах из T . Оно ляжет в начало (счётной) последовательности из множеств, $D_0 \subseteq D_1 \subseteq D_2 \subseteq \dots$, объединив которую мы получим множество D^* , которое и будет требуемым предметным множеством.

Заметим, что в результате однократного процесса пополнения мы увеличим множество D' не более чем на $|T| \cdot \aleph_0 \cdot |D'|$ элементов (по каждой формуле по каждой константе из D' добавим не более, чем конечное количество элементов). Поэтому мы не выйдем из мощности $|T|$, если T несчётно, или из \aleph_0 , если T — конечно. Значит, мощность D^* также будет отвечать условию теоремы.

Часть 2. Покажем, что структура M^* , полученная сужением модели M на предметное множество D^* , является элементарной подмоделью. Докажем это индукцией по структуре формул. Рассмотрим некоторую формулу $A(x_1, \dots, x_n)$, при этом $x_i \in D^*$.

База. Эта формула — предикат $P(f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n))$. Если x_1, \dots, x_n взяты из D^* , то все они добавлены на некотором шаге, значит, найдётся такой t , что $x_i \in D_t$. Значит, все результаты функций $f_j(x_1, \dots, x_n)$ лежат в D_{t+1} . Значит, формула будет определена на этих значениях. Очевидно, что истинность (ложность) формулы сохранится.

Переход. Пусть есть некоторая формула A — связка одной или двух подформул, и A имеет следующий вид:

1. $X \& Y, X \vee Y, \neg X, X \rightarrow Y$ — ясно, что все эти правила работают на сужении исходной модели, и истинность формулы сохраняется.
2. $\exists y B(y, x_1, \dots, x_n)$. Фиксируем некоторый набор x_1, \dots, x_n из D^* . Пусть формула A истинна в M , покажем её истинность в M^* . Заметим, что каждый из x_i был добавлен в D^* на конкретном шаге, то есть найдётся такой номер t , что все x_i принадлежат D_t . Тогда, по построению множества D_{t+1} , в нём неизбежно найдётся такой y , что $B(y, x_1, \dots, x_n)$ определено и выполнено в M . Значит, B будет выполнено и в M^* (по предположению индукции). Значит, A истинна и в M^* . Обратное также очевидно: если y найдётся в узкой модели, то он тем более найдётся в широкой.
3. $\forall y B(y, x_1, \dots, x_n)$. Доказательство зеркально соответствует предыдущему пункту. Истинность $\forall y B(y, x_1, \dots, x_n)$ в M очевидно влечет истинность $\forall y B(y, x_1, \dots, x_n)$ в M^* , так как $D^* \subseteq D$. Если же $\forall y B(y, x_1, \dots, x_n)$ ложно в M , то существует такой y из D ,

что $\neg B(y, x_1, \dots, x_n)$ истинно в M , значит, по построению D^* и в нём найдется элемент z с таким свойством, то есть $B(z, x_1, \dots, x_n)$ ложно в M . И по предположению индукции $B(z, x_1, \dots, x_n)$ ложно в M^* . То есть $\forall y B(y, x_1, \dots, x_n)$ ложно в M^* .

□

Данная теорема в частности показывает, что для теории множеств (очевидно, счётно-аксиоматизируемой) имеется счётная модель. В частности, это приводит к следующему утверждению, называемому *парадоксом Сколема*: для любого множества, определимого в аксиоматике Цермело-Френкеля, мы можем предложить способ перенумеровать его элементы натуральными числами. В том числе это справедливо и для несчётных множеств — то есть для тех множеств, для которых доказано отсутствие этого способа.

Парадокс, тем не менее, здесь кажущийся, поскольку тут (некорректно) сталкивается утверждение, формулируемое на предметном языке (об отсутствии способа пересчёта внутри теории), с утверждением на мета-языке (о существовании этого способа вне теории).

14 Литература

Возможно, в ходе подготовки вам потребуются дополнительные источники. В таком случае рекомендуется использовать следующие книги:

- Классическое исчисление высказываний и предикатов:
С. Клини. Математическая логика — М.: Изд-во «Мир», 1973
Н.К. Верещагин, А. Шень, Лекции по математической логике и теории алгоритмов, Языки и исчисления — МЦНМО, 2002. Также доступно по ссылке <http://www.mcsme.ru/free-books/shen/shen-logic-part2.pdf>
- Интуиционистская логика:
Н.К. Верещагин, А. Шень, Лекции по математической логике и теории алгоритмов, Языки и исчисления — МЦНМО, 2002. Также доступно по ссылке <http://www.mcsme.ru/free-books/shen/shen-logic-part2.pdf>
- Теорема Геделя о неполноте арифметики:
Э. Мендельсон. Введение в математическую логику — М.: Изд-во «Наука», 1971.
- Теория множеств:
А.А. Френкель, И. Бар-Хиллел. Основания теории множеств — М.: Изд-во «Мир», 1966.
П.Дж. Козн. Теория множеств и континуум-гипотеза — М.: Изд-во «Мир», 1969.